STATEMENT OF THE HONORABLE JOHN T. SPOTILA
ADMINISTRATOR
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
July 26, 2000

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here to discuss Administration efforts in the areas of computer security and associated critical infrastructure protection. We know that our government and our nation rely increasingly on computer systems to support nearly every critical governmental and business function. Government and industry are now more interconnected than ever, operating in a shared risk environment, with our interdependence growing daily. The integrity and availability of our systems and, where appropriate, the confidentiality and privacy of information in those systems are today more important than ever.

Administration Actions

The President has given high priority to cyber security and the protection of our nation's critical information assets. He understands the growing risks that our nation faces from cyber threats. In May 1998, after reviewing the report of his Commission on Critical Infrastructure Protection, he issued Presidential Decision Directive 63, on "Critical Infrastructure Protection."

This Directive provided a framework for government action. It pointed out that interconnected computer systems are necessary for the provision of essential national services. It recognized that a potential future attack against the United States might take the form of a cyber attack against our critical computer systems. It acknowledged that government and industry face essentially the same risk in this area and must work in close partnership to mitigate that risk. Indeed, as today's hearing also recognizes, it took into account that this risk is shared

globally.

The Directive also called on all Executive branch agencies to assess the vulnerabilities to their systems and the nation's critical infrastructures -- communications, energy, banking and finance, transportation, emergency services, and public health. It placed special emphasis on protection of the government's own critical assets and establishing the government as a model for information security. This is where OMB's primary role lies and where we have been concentrating our efforts.

To implement the Directive, the President appointed Richard Clarke of the National Security Council as the nation's first National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. Later, the National Security Advisor announced the appointment of Jeffrey Hunker as Senior Director for Critical Infrastructure Protection, in the Office of Transnational Threats. Both have worked tirelessly to increase national awareness of the scope of the problems in this area, working closely with OMB to help formulate sound approaches to addressing these problems.

The Directive called for the development of a detailed National Plan for Information Systems protection, so that we could better defend against cyber disruptions. It also established a Critical Infrastructure Assurance Office (CIAO) at the Department of Commerce to coordinate government interaction with industry, develop the national plan, and assist federal agencies in identifying and prioritizing their own critical assets.

The Directive also established at the FBI the National Infrastructure Protection Center (NIPC) as a national focal point for gathering information on threats to the nation's critical infrastructures. The NIPC's Director, Michael Vatis is also testifying before you today.

In January of this year, the President announced the issuance of version one of the National Plan for Information Systems Protection. He pointed out that the Plan was the first major element of a more comprehensive effort and that it would evolve and be updated as we increase our knowledge of our vulnerabilities and of emerging threats. The plan called for a number of government-wide and agency-specific security initiatives, as well as increased cooperation with industry and others in the private sector. In this last regard, we note that CIAO under the leadership of its Director, John Tritak, has worked with industry to build the Partnership for Critical Infrastructure Security, now comprising more than 130 representatives from major U.S. corporations. The Partnership is

meeting this week in San Francisco.

In February of this year, in the wake of a series of distributed denial of service attacks against a number of major electronic commerce websites, the President held a Cyber Security Summit with key information technology leaders. At this summit, which I attended, the private sector leaders emphasized their desire to participate in partnerships with the government and with one another to facilitate the sharing of information on cyber attacks and common vulnerabilities.

The President's Chief of Staff, John Podesta, has been personally engaged in these security issues. He has directed the agencies to take specific actions to improve security and to report to him on the status of the security posture of their websites. Just last week, he delivered a major speech outlining the Administration's position on cyber crime legislative reforms designed to upgrade 21st Century law enforcement capabilities and also enhance privacy and civil liberties in cyber space.

The President's FY 2001 budget proposed approximately $2.0 billion for agency critical infrastructure protection and computer security programs out of a total information technology budget of about $40 billion. This security total is a 15% increase over the FY 2000 enacted total of $1.8 billion. It includes funding to help detect computer attacks, coordinate research on security technology, hire and train more security experts, and create an internal expert review team for non-defense agencies. These initiatives are vitally important.

Regrettably, many of our requests for security funds face an uncertain future in the appropriations process. It has been particularly difficult to gain support for cross-cutting initiatives, despite their importance to our computer security efforts. We should be more open to innovative approaches in this area and look for opportunities for synergy and interagency cooperation.

Several important cross-cutting government initiatives are at risk in the appropriations process, but can still be salvaged:

Department of Commerce

- $5 million at the National Institute for Standards and Technology (NIST) to establish an expert security review team to help agencies review their systems and programs, identify unacceptable risks, and assist in mitigating them. This program would operate in the context of NIST's statutory responsibilities under the Computer Security Act of 1987 and Clinger-Cohen Act of 1996 to issue security

guidance to the agencies.

- $50 million to create the Institute for Information Infrastructure Protection at NIST. The Institute would work collaboratively with industry and academia to fill research and development gaps for key security technologies. Industry often has no incentive to invest in long-term research and development without a clear market need. Research would be performed at private corporations, universities, and non-profit research institutes.

General Services Administration

- $5.4 million to maintain the Federal Computer Incident Response Capability (FedCIRC), the central government non-law enforcement focal point for responding to attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. A portion of this funding will also continue government support of Carnegie-Mellon University's highly acclaimed Computer Emergency Response Team (CERT).

- $10 million for next generation intrusion detection. This funding would be used to establish the Federal Intrusion Detection Network (FIDNet) which would complement FedCIRC by standardizing ongoing agency computer intrusion detection activities, automating many of the cumbersome manual processes now employed, and providing a centralized expert analytic capability that does not exist at most agencies.

Department of Treasury

- $7 million at Treasury to complete the development of an interoperable government-wide infrastructure to permit authenticated electronic transactions and thus promote the electronic delivery of services to the public. In our traditional, paper-based world, government, industry, and the public rely on trusted and verifiable relationships, photo IDs, notarized signatures, and face-to-face contact to authenticate one another's identity prior to conducting business. We need a similar authentication capability in our new electronic world. This funding would translate paper-based relationships into similar trusted and verifiable electronic relationships.

Office of Personnel Management and the National Science Foundation

- $7 million at the Office of Personnel Management and $11.2 million at the National Science Foundation for Federal Cyber

Services/Scholarships for Service. The Scholarship for Service effort will help develop the next generation of Federal information technology managers by awarding scholarships for the study of information assurance and computer security in exchange for Federal Service.

OMB's Role in Government Computer Security

In February, OMB Director Jacob Lew issued important guidance to the agencies on incorporating security and privacy requirements in each of their FY 2002 information technology budget submissions. In the future, when requesting approval for information technology funds, agencies must demonstrate how they have built adequate security and privacy controls into the life-cycle maintenance and technical architectures of each of their systems. Without an adequate showing, the systems will not be funded.

Let me use this point to illustrate OMB's role in computer security and put it in the context of today's hearing. While OMB does have a broad, government-wide role in formulating the President's budget, promoting the effective agency use of agency resources, and promoting sound agency management practices, including oversight of the use of agency information resources, our specific role for security is limited to policy development and oversight for unclassified government information and computer systems. We have no direct role in law enforcement or international affairs. While we maintain a close relationship with operational agencies, we have no operational responsibilities ourselves.

We are very much committed to the protection of Federal computer systems. We recognize that security, or information assurance as it is sometimes called, consists of a number of separate components:

- Confidentiality -- assuring that information will be kept secret, with access limited to appropriate persons for authorized purposes;
- Integrity -- assuring that information is not accidentally or maliciously altered or destroyed, that systems are resistant to tampering, and that they operate as intended;
- Availability -- assuring that information and systems will be ready for use when needed;
- Reliability -- assuring that systems will perform consistently and at an acceptable level of quality; and

- Authentication -- assuring that users of systems and parties to transactions are verified and known so that the sender knows that data has been delivered and the recipient knows the sender's identity. With authentication comes nonrepudiation, since neither party can later deny having sent or received the data.

The Legal Framework

Congress has provided a sound legal framework for the Executive branch to address computer security needs. OMB has built on this statutory framework. Relying on our general authority, we issued our first computer security policy in 1978. That policy defined a minimum set of controls for the security of Federal automated information systems tailored to the processing environment of its time -- a centralized environment running mostly custom-developed application software. In 1985, we updated that guidance as part of new, comprehensive guidance on information resources management, OMB Circular A-130. Appendix III of A-130, "Security of Federal Automated Information Systems," began to address the security vulnerabilities introduced by remote processing -- which at that time occurred largely through dial-up communications.

Today's computing environment is significantly different. It is characterized by open, widely distributed processing systems using commercial off-the-shelf software. While effective use of information technology often reduces risks to Federal programs (for example, reduced risks from fraud or errors), the risk to and vulnerability of Federal information resources has increased. Greater risks result from increasing quantities of valuable information being committed to Federal systems, and from agencies being critically dependent on those systems to perform their missions. Greater vulnerabilities exist because so many Federal employees have access to Federal systems, and because these systems now interconnect with outside systems and the Internet.

Two years after the issuance of Appendix III to Circular A-130, Congress enacted the Computer Security Act of 1987 (P.L. 100-235) requiring agencies to improve the security and privacy of Federal computer systems, plan for the security of sensitive systems, and provide mandatory awareness and training in security for all individuals with access to computer systems. The Computer Security Act established the National Institute for Standards and Technology (NIST) as having the lead in setting standards for the security of unclassified Federal information technology.

The Paperwork Reduction Act (PRA) of 1995, P.L. 104-13, then established a comprehensive information resources management framework which subsumed preexisting agency and OMB responsibilities under the Computer Security Act. It recognized our transition to an increasingly internetworked information environment, and the security and privacy challenges which go along with that transition.

OMB revised Appendix III to Circular A-130 in February 1996 to address specifically the computer security mandate of the 1995 PRA. The revised Appendix updated policies and set responsibilities for the security of Federal information systems including the confidentiality, availability, and integrity of information and systems.

Overall, OMB Circular A-130 sets forth government-wide polices for a wide variety of information and information resource management issues. The body of the Circular addresses agency management of information and information systems including capital planning and investment control. Appendix I sets privacy policy. The soon to be issued Appendix II defines policy for information architectures and implementation of the Government Paperwork Elimination Act. Appendix III sets security policy. In Appendix II -- our guidance on the Government Paperwork Elimination Act -- we address the authentication and nonrepudiation elements of security mentioned earlier.

Appendix III implements another Computer Security Act requirement by directing the Department of Commerce (through NIST) to issue appropriate security standards and guidance, update security training guidelines, provide guidance for security planning, provide guidance and assistance to Federal agencies on appropriate security when interconnecting with other systems, coordinate agency incident response activities, evaluate new technologies, and apprise Federal agencies of their security vulnerabilities.

Importantly, Appendix III also requires Federal agencies to adopt a minimum set of risk-based management controls. Four controls are described: assigning responsibility for security; security planning; periodic review of security controls; and management authorization. These controls are intentionally not technology dependent. Instead, they focus on the management controls agencies need to assure adequate security of the information technology now in the hands of millions of Federal users. Technical and operational controls should support these management controls.

More recently, the Information Technology Management Reform Act of 1996 P.L. 104-106 Div. E (Clinger-Cohen Act) linked OMB

and agency computer security responsibilities firmly to agency information resources management, capital planning, and budget processes. It established agency Chief Information Officers who report to agency heads as the responsible focal point for agency information resources management, including security. Agency CIOs are responsible for oversight of the security policies and practices embodied in the Computer Security Act, the Paperwork Reduction Act of 1995, and OMB Circular No. A-130. These responsibilities include the need for explicit consideration of security requirements in the development of agency information technology architectures and the need to ensure appropriate levels of security awareness and training.

The Clinger-Cohen Act tied agency information resource management responsibilities, including security, to the capital planning and budgetary oversight process the agency engages in with OMB. When OMB reviews information technology investment plans generally, or when it examines specific major information systems, it evaluates agency security planning and practices. This reflects the influence of Clinger-Cohen.

Lastly, Clinger-Cohen recodified and highlighted Commerce's computer security responsibilities, particularly in the area of standards and guidelines. The Act underscored the requirement for agencies to ensure that their security planning was consistent with the standards and guidelines developed by NIST. NIST issued comprehensive security planning guidance in December 1998.

In 1998, the Government Paperwork Elimination Act (the Paperwork Elimination Act) addressed OMB and agency responsibilities for conducting business in an electronic environment. It required that agencies provide for the optional use and acceptance of electronic documents and signatures, and introduce electronic record keeping when practicable. It provided that electronic records and their related electronic signatures must not be denied legal effect, validity, or enforceability merely because they are in electronic form. It also contemplated Federal acceptance of a range of electronic signature alternatives. By October 21, 2003, agencies must have electronic filing and electronic signature capabilities in place. OMB published its guidance on implementing the Act in the Federal Register on May 2nd 2000. The guidance describes the methods agencies can use to provide for the authentication of digital signatures.

Are current policies effective?

In reviewing our recent efforts in the area of computer security, OMB has taken a close look at the effectiveness of our

current policies. In general, we believe that our policies and guidance for unclassified applications are adequate, although some updating and additional detail would be helpful. We plan to provide additional detail in our upcoming revision to these policies. Indeed, reports from GAO, including its assessment of security practices of leading private sector organizations, show that OMB policies and NIST guidance are properly focused on a risk-based, cost effective approach and reflect the right balance between strong security and mission needs.

As discussed earlier, OMB Circular A-130 establishes an overall framework for government information and information resource management. We must integrate security within this framework to ensure that it remains cost-effective, forms an integral part of agency business processes, enables rather than impedes agency missions, and operates effectively over time.

How can we ensure effective policies?

We recognize that security measures must function effectively in the real world of agency missions and business operations. To accomplish this, we focus on a number of key principles:

- We should consider widely diverse views and attempt to accommodate unique agency needs. Agency information management practices often affect the public, industry, and state and local governments. In considering new approaches to security we need an open and transparent process that encourages and makes good use of public comment.

- Although the views of the general security and national security community are essential in developing sound security policy, they are not the only ones we should consider. Agency CIOs, program officials, and others also have important perspectives and their views are essential in the policy development process.

- Ultimately, the responsibility for security of systems and programs should lie with each agency and with the specific program officials in each agency. Unless we develop policy that fits within that context, security will become an afterthought.

- Compliance always improves when we build security into our systems and work processes in close coordination with the program officials that are closest to the affected operations.

- Funding and managing security apart from a program

encourages program officials, system owners and users to ignore it. Separation sends a signal to them that security is not their job. If program officials and users do not take responsibility for security, then security officers and others must do so, often by employing resource intensive compliance inspections. This approach carries risk since the only time one knows the level of compliance is during or immediately following an inspection.

Good design and good planning are the keys to successful security. They are the keys to successful security. For good design, security must be compatible with and enable -- not unnecessarily impede -- system performance, business operations, and the mission. When security unnecessarily slows the system or hinders the mission, users often work around it or ignore it completely. To work effectively, security must be part of the system architecture, built-in so that users will "buy-in."

Good planning requires that we fund security and privacy as part of the life-cycle costs for each system. To identify true system costs and adequately plan for future system or program operations, we must account for all of the resources necessary to operate the systems, including security. Indeed, attempting to fund security independent of the program or system within which it lives makes it far more difficult to build a business case for the security component. If it isn't tied to the mission, how can one demonstrate security's support of the mission?

Our approach provides maximum flexibility for agencies so that they can make appropriate, informed choices in applying necessary security controls that are consistent with their unique circumstances. It minimizes conflicts that could easily arise from any centralized approach to widely diverse agencies with a broad range of varied and shifting requirements.

How can we improve compliance?

As GAO, our agency Inspectors General, our own program reviews, and industry and private security experts all agree, most security problems come not from a lack of policy, but rather from ineffective or incomplete implementation of existing policies and guidance. We are very much aware of this risk in the Federal context. In government, ineffective implementation can arise from inadequate resources, lack of management attention, and inadequate employee training. In the past few years, a great deal of agency management attention focused on Y2K remediation, drawing on agency resources and delaying full implementation of the Clinger-Cohen approach. There is much more to be done before we reach full implementation of our existing security guidance.

We believe agencies must meet the following three goals to ensure successful security policy implementation:

- They must achieve consensus and get user buy-in when initially setting policy so that the product will be better.

- They must tie security to their capital planning and investment control process and to their budgets.

- They must establish and maintain senior management support.

OMB will do all that it can to encourage and help the agencies in these efforts.

To identify specific problems regarding implementation, we are collecting empirical data from the agencies. We began in June 1999 with a systematic review of agency risk management processes. We are now focusing on the security posture of 43 high impact government programs such as Medicare, Medicaid, the Air Traffic Control System, Social Security, and Student Aid.

Our findings to date are illuminating. Agencies need to improve their integration of security into their capital planning and investment control processes. As mentioned earlier, in February of this year, we provided the agencies with the first step towards a solution -- specific security criteria that agencies must meet before they receive FY 2002 funding for information technology investment requests. These criteria require agencies to demonstrate explicitly how their information technology investments provides for adequate security controls and how they account for the costs of those controls over the life of each system.

Additionally, OMB's budget preparation guidance to the agencies this year will add a requirement that they include, for each system, a percentage amount for security. Over time, we believe this will give us better information on true security costs.

Cross-Cutting Efforts

We are working with the NSC, the CIO Council, NIST, GSA, GAO, and others on a number of specific projects to assist the agencies and enhance government-wide security. These include:

- Testing a systematic process of identifying, assessing, and sharing effective security practices. The CIO Council has developed a searchable database and website to facilitate this activity.

- Finalizing security performance measures (metrics) against which agencies can assess their security programs and take steps to mature them over time. Agency comments on the final draft of this assessment framework are due this week. NIST and the CIO Council are scheduling a workshop for August to discuss the comments broadly. It is significant to note that our assessment framework compares favorably with the results of a similar effort by a major financial institution widely recognized as an industry leader in security.

- Creating a formal process for coordinating the government-wide response to cyber incidents of national significance. This process includes the formation of a working group consisting of OMB, the FBI, Departments of Justice, Defense, and Commerce, the intelligence community, GSA, and the CIO Council, along with a senior level steering group consisting of senior officials from the above agencies, the NSC and OSTP.

- Improving the operational effectiveness of the Federal Computer Incident Response Capability (FedCIRC) in responding to lower level incidents and coordinating federal agency sharing of information regarding common vulnerabilities and computer incidents. Several years ago, OMB designated FedCIRC as the primary avenue for agencies to fulfill their information sharing responsibilities. OMB and the CIO Council are working together to enhance that capability.

- Using the FedCIRC organization to promote more timely agency installation of patches for known vulnerabilities. Many successful attacks against government and industry systems have been the result of old vulnerabilities for which vendor patches are readily available at no cost. Installing such patches is not, however, a trivial task; it requires considerable time and effort on the part of systems administrators who often are busy just keeping their systems up and running efficiently. We hope to provide some relief through this cross-cutting initiative if we can obtain necessary future funding.

- Reviewing security policies and practices of the national security community to see if they have applicability for those agencies that operate in an unclassified environment. Where appropriate, those policies and practices will be adapted for general agency use.

- Exploring with the CFO Council the viability of establishing a security benchmark or standard expectation for the

security of agency financial systems. This effort may prove to be an effective pilot for establishing similar benchmarks for other discrete classes of information and systems. At the same time, we want to move carefully in this area to avoid the temptation to establish one-size-fits-all security requirements.

- Developing a government-wide Public Key Infrastructure (PKI) – a trusted digital signature infrastructure that will facilitate a broad range of services including tax filings, regulatory submissions, student and small business loans, benefit applications, grants, and many more. The PKI will be essential to agency implementation of the Paperwork Elimination Act. The Federal PKI Steering Committee, sponsored by the CIO Council, is working with government agencies and industry to field a comprehensive network-based infrastructure to support a federal PKI. Part of this task involves allowing digital signatures from different government agencies and different vendors to interoperate. A pilot, "Certificate Bridge Authority" successfully tested this interoperability in April and will be operational later this year. The PKI, through digital signature services and encryption, provides four of the basic security services I mentioned earlier -- confidentiality, integrity, authenticity, and non-repudiation. For all of these efforts, adequate future funding will be essential.

These are innovative efforts that show great promise. They need Congressional support if we are to fulfill that promise.

New Legislation

On a current note, we are very supportive of the Government Information Security Act of 2000, now part of the pending FY 2001 Defense Authorization Act. The Administration worked closely, in a non-partisan way, with the authors of this legislation. We share a desire to meet the security needs of the government and promote security as an essential management function. The Federal government has come a long way since the original Computer Security Act was passed in 1987. There have been significant technology and policy changes along the way. If it becomes law, the Government Information Security Act will update our statutory framework in a thoughtful and constructive manner.

Conclusion

We appreciate your interest in all of these matters and look forward to continuing our close cooperation with the Committee in this important area. We value our partnership with you and hope that this hearing will mark a further strengthening of our joint

efforts on behalf of the American people.

Thank you.